

.....

---

# **Internet2 Early Adopters Project**

.....

## **Scoping Document for Michigan Technological University**

**September 25, 2000**

---

# Table of Contents

<b>Readiness study.....</b>	<b>3</b>
<b>Project background information.....</b>	<b>4</b>
<b>Project statement or goals .....</b>	<b>6</b>
<b>Strategy and staging.....</b>	<b>7</b>
<b>Key deliverables and/or features.....</b>	<b>11</b>
<b>Evaluation or comparison of competing solutions .....</b>	<b>11</b>
<b>Boundaries and constraints.....</b>	<b>12</b>
<b>Role of external specialists or consultants .....</b>	<b>12</b>
<b>Key project issues and risk assessment.....</b>	<b>13</b>
<b>Contingency plan and mitigation measures .....</b>	<b>14</b>
<b>Resources .....</b>	<b>14</b>
<b>Primary contact person or liaison.....</b>	<b>15</b>
<b>Project champion or sponsor .....</b>	<b>15</b>
<b>Communication plan.....</b>	<b>15</b>
<b>Appendix A: Early Adopters Team at Michigan Tech .....</b>	<b>16</b>

# Scoping Document for Michigan Technological University

## Readiness study

Michigan Technological University is a public, Doctoral II research university located in the Upper Peninsula of Michigan. The Institution's enrollment is approximately 6,000 students, ten percent of whom are graduate students. Roughly sixty percent of the student body is enrolled in engineering programs.

### Conditions for readiness

The Information Technology organization determined that the campus was ready to begin implementing directory services and campus-wide authentication services in the past year. Key conditions for this decision include the following.

- **Organizational Model.** Michigan Tech has a hybrid support model. The central information technology organization assists departmental system administrators and maintains the master campus servers, entire network infrastructure, institutional data, and applications infrastructure. Each department is responsible for providing desktop computers, departmental servers, local applications, and the personnel to support their additional needs. The glue that makes this work is our commitment to using network and applications standards (TCP/IP, SMTP, MIME, etc.) coupled with a technical group called the System Administration Council. This open committee, which includes Information Technology (IT) staff and department technical staff, develops technical standards and provides a campus communication and support forum.
- **Unique Identifier.** We have a campus unique identifier based on the PIDM (the SCT Banner identifier). To receive an account on campus, a user must be entered into the SCT Banner system and is then issued a PIDM number. This number is unique for each individual and is not reused or recycled. All logins, both primary and secondary, are linked in our Network Information Database for ownership and responsibility via their unique PIDM. The users PIDM is also placed on their Michigan Tech identification card and is used to track meal plans and access to campus parking lots and buildings via ABA magnetic stripe readers.
- **Directory Services.** We developed an LDAP-based directory service and person entry containing information such as login, PIDM, name, campus card picture, etc.
- **Institutional Data in Oracle.** Campus mission-critical data resides in Oracle. This includes the administrative data and information about people and devices deployed on, and connected to the campus network and phone.
- **Internet2 Commitment.** Michigan Tech joined Internet2 and connected to the Abilene network in fall of 1999. At that time, we began working with the faculty to actively develop applications and partnerships at other institutions. Enabling inter-institutional

collaboration is becoming critical as more faculty participate on teaching and research teams across the nation.

- **Policy and Political Climate.** Michigan Tech has a well-developed technology advisory committee structure that we have had in place for over ten years. Included in this structure are subcommittees addressing standards, student computer fees, planning, acquisitions, security, and system administration. The representatives constitute a broad constituency of the campus, including IT.

Michigan Tech assembled a faculty Internet2 Advisory Committee that promotes the use of our connection, as well as recommends policy on its use. We also have an administrative committee that reviews, recommends, and implements policy regarding our administrative data. On this team are functional leads from all administrative areas, including Office of Student Records and Registration, Alumni, Financial Aid, Human Resources, and so on. These departments have been using this process for decision making for over eight years.

## Project background information

### Rationale

Michigan Tech collaborates with other institutions, researchers, and colleagues across the world and offers services to an extended campus family of remote students, parents, alumni, and friends. MTU continues to seek ways to enhance this collaboration and nurture these on an on-going basis, regardless of location or time constraints.

Technology can provide this collaboration vehicle through the deployment of Internet-based access to information and services. Explicit in the architecture is the concept of security and flexibility creating an environment that is both mindful of and tailored to the needs of those using the applications. It is our belief that using standard, object-oriented, portable, and secure technologies will enable the University community to interact effortlessly without the traditional constraints of location, time, and platform.

### Motivating factors and drivers

Information access and the information economy are driving higher education to change. In addition to addressing the rising expectations of our students, faculty, and staff, Michigan Tech would like to offer more services to friends and corporate partners. Our driving forces include:

- Requirements for interdisciplinary and inter-institutional research
- Fund raising and space constraints
- Curriculum reform and flexible teaching methods
- Constituents' escalating expectations for the pervasive access to, and use of, technology
- Revenue opportunities with offering education at a distance
- Fast company changes and anticipation of the information economy of the 21<sup>st</sup> century

A number of issues appeared, which solidified Information Technology's resolve to implement the initial middleware components. We found that to respond adequately to these forces we need to

- **Manage information about, use of, and access to electronic resources.** Michigan Tech's WAN connection traffic has tripled in the last year. Although no one wants to limit our network use, we know that at some point we will need to set priorities for

applications and use. For instance, an instructor may need a guaranteed amount of bandwidth for a one-hour videoconference. We should be able to fulfill this request.

- **Develop a normalized repository of institutional data and objects.** Although we have the majority of our institutional data stored in Oracle (library, administrative systems, network information and the like), there was no roadmap regarding which address type to use. MTU needed a source of commonly used information for developing local and campus applications. In addition, we will not be able to increase our staff to accommodate older methods of development, given the funding needs in the academic areas. We have to streamline our development process to reduce the deployment and maintenance time.
- **Secure our authentication process.** Our passwords travel over the network unencrypted. We have a knowledgeable student body and a very active residential network. Many new departmental system administrators often don't have the same security knowledge as experienced technical staff. These factors combined increase our security risk greatly.
- **Provide a secure and easy access to the campus electronic services.** Because many faculty and staff travel, they would like a method to connect back to campus, read e-mail, and access files and applications. Students who are away from the campus, during break times or on co-op, would like to be able to communicate with their peers electronically.

### **Justification and consequences**

Additional justification for this project can be found under the section entitled *Motivating Factors and Drivers*. Consequences of *implementing* this project include:

- Increased cost in software and hardware maintenance to support directory services. This cost is incurred by IT.
- Increased time spent by system administrators to change their current configurations and work with peers to implement security and application deployment practices.
- Additional data custodian and technical staff time to manage and guide the use of the directory service.
- Better communication within the data and technical community.

However, the short and long-term consequences of *not implementing* directory services and campus authentication are much greater:

- Lack of ability to share secure electronic resources among institutions connected to Internet2 initially, and organizations connected to the commodity Internet in the longer term. Lack of ability to access similar resources offered by other schools. This will be an issue of importance to faculty collaborating with other researchers and instructors.
- Increased complexity in deploying secure electronic services to the campus and managing access to them. Without a standardized data look-up service and authentication model, the technical staff will be maintaining local pockets of duplicated data and separate authentication systems across the institution. This will increase our collective maintenance costs substantially.
- Increased risk of security breaches without a consistent model for access and password management.
- Increased costs to implement business requirements quickly, such as responding to a new data privacy law.

### **Connections to other institutional priorities or mission(s)**

Michigan Tech will move from a tethered, location-dependent computing environment to a flexible, location-independent, information environment in the next three to five years, which is characterized by the following:

- Researchers will collaborate with colleagues across the globe.
- Faculty, staff, and students will seamlessly access their information and applications from a variety of information appliances.
- Resources and environments will follow students, faculty, and staff.
- Secure and trusted access will be available on and off campus for collaborating faculty, students, and staff.
- Michigan Tech will enter into consortiums with the goal of sharing costs of expensive licenses for library, data, and application resources.
- Instructors will be able to seamlessly incorporate on-line content developed by faculty at other institutions.
- Michigan Tech will maintain solid contact with our friends, partners, and alumni; and offer them tailored electronic services.

A prerequisite for implementation is the sharing of institutional data about our students, faculty, and staff, along with information about what they are authorized to do. It requires tracking their access and preferences, and offering services where they know their information is confidential. In short, it requires us to build directory, authentication, and authorization services, as well as secure connections to them.

## **Project statement or goals**

The goal of the project is to develop the initial infrastructure needed to more quickly deploy secure, network and Internet-based applications. In addition, we intend to participate in the development of best practices for this infrastructure with the national Early Adopters Project members and together develop some shared basic applications. This infrastructure, or middleware, is a suite of services used by both a network and network applications in the form of data look-up, authentication, and security. For more information on Michigan Tech's project, refer to <http://www.ea.mtu.edu>.

### **Project Methodology**

To help ensure a successful implementation, we will use the following philosophy:

- Deploy several applications important to key constituents that demonstrate the need for middleware. Applications will drive the infrastructure implementation.
- Work with campus technical and data staff. Getting the campus System Administration Council on board is a critical component to success. They will be implementing the distributed components in the departments and are knowledgeable about what does and doesn't work in their environment.
- Simplify, automate, and model the processes and architecture. The process for changing and using these services must also be designed and deployed.
- Implement newer technology where practical and appropriate.
- Document models, processes, designs, and interactions.

### **Stakeholders or constituents**

In the short term, our stakeholders consist of data owners/custodians and technical staff across campus. The data custodians must be satisfied that the data in the directory is being used and loaded appropriately. The technical staff must understand why we are implementing middleware, since it is they who will be assisting us and communicating back to the faculty, staff, and students about the project. In the future, they may also find the services useful to their own local applications.

Trailblazing faculty are also stakeholders in this project, because they use cutting-edge technology in their instruction and research.

IT is also a stakeholder with their services they would like to offer to the Michigan Tech community. In the longer term, the stakeholders will also include to the faculty, staff, and students, such as Internet2 researchers and Financial Aid recipients.

## Strategy and staging

The scope of the first two stages is limited to implementing high-visibility target applications and the infrastructure needed to support them. In essence, we are designing with the global issues in mind, but using the applications to push the prototyping and acceptance of the architecture. As of the writing of this document, we are nearing the end of the first stage, or the short-range strategy.

### Short-range strategy

This project stage is focused on educating each other, reviewing campus identifiers, deploying production directory and time services, and implementing several applications to use this new service. This first phase of the project has a target completion date of November 1, 2000.

### Deployment constraints

Due to time and personnel restrictions, stage 1 is under a few deployment constraints. Because our directory service is immature at this point, we will use it for applications that are not mission-critical. In doing so, we can work out any issues with feed scripts and error handling, for example, without putting the institution at too much risk.

The unique identifier strategy will be subject to overall project priorities and external needs. Our existing model works for the short-term.

### Project components

#### Team member education

In addition to providing reference documents and access to the Burton Group site, we also demonstrated the overall issues surrounding middleware deployments by picking one application to implement on paper. To do this, we created one subteam of the data and policy members and another subteam consisting of the technical members. Each team addressed their aspect of the application and reviewed issues such as authentication, security, data ownership and integrity, and so on. We then had a group discussion on the combined issues.

#### Unique identifier strategy

The project team reviewed identifiers on campus to decide whether action would be needed. Michigan Tech, as noted earlier, uses our SCT Banner PIDM as our unique identifier for faculty, staff, students, and alumni. Currently, visitors also receive a PIDM if they need to access buildings or receive a computer account. When more of our electronic services are offered to broader audiences, such as corporate partners, prospective students, and collaborating researchers, we may need to develop another mechanism to track them.

#### Production directory service

We installed iPlanet's directory service and have been running it since summer of 1999. However, to bring the service to full production, a number of items were addressed.

- Final schema was designed and implemented.

- Public and private data and access methods were defined and implemented.
- Robust feed method was implemented and monitored.
- Initial documentation still needs to be finished regarding the service, schema, attributes, and their characteristics.

#### Time Services

Coordinating time between clients and servers on a computer network is extremely important. Authentication, authorization, network file systems, and distributed computing all depend on accurate time synchronization for optimum performance.

MTU currently relies on the CoBox Network Time Server from Lantronix to ensure time synchronization across the network. The device contacts a Global Positioning Satellite for a standard time source and makes that timing information available to all other devices on the network via Network Time Protocol.

#### Application projects

##### 1. Photo roster

Michigan Tech began to distribute photo rosters to instructors in the fall quarter of 1999. This application relies on the directory server to provide student photos for approximately 6000 students enrolled at MTU. The application reads the information from a relational database to obtain a list of registered students for a given class. Once this list is built, the directory server is queried to acquire each student's picture. Currently, we print these rosters and distribute them to the faculty. In the long term, we plan to move this application to the Web and use LDAP-based authentication.

##### 2. E-kiosk services

We developed a kiosk to offer the following services by fall of 2000:

- Distribute a Kerberos password to students, faculty, and staff who wish to access the public modem bank. This is a temporary application and will not be needed when we move to LDAP-based authentication for the modem bank.
- Collect chip identifiers on our campus TechExpress smart card. We developed a system for collecting, storing, and associating it with the student's account information for use in Sun Microsystems Sun Ray thin client. Once a student inserts the TechExpress card into the smart card reader on the Sun Ray, we use the chip id as the identifier to retrieve his or her account. This is a temporary application and will not be needed after we collect the returning students' chip identifiers. Future chip ids will be collected at card distribution.

These kiosks have touch screen menu systems, which guide students through the applications. Information pertaining to the user (login, name, picture, etc.) is obtained through the campus directory server.

##### 3. Dynamic Host Configuration Protocol (DHCP)

The DHCP component allows machines such as thin-clients to boot across subnets. We have implemented a DHCP relay topology that does the following:

- Localizes DHCP broadcast traffic to an individual subnet (i.e., MTU does not route broadcast traffic between subnets).
- Allows for redundant DHCP master servers. These servers may reside on the same subnet, or on different subnets, as all DHCP requests to the masters are point-to-point via a DHCP relay.

- Provides a highly available DHCP service. Because the DHCP relay can forward requests to a list of DHCP servers, a request will be forwarded to the next server in the list if one of them is not responding.

For example, a Sun Ray thin client will broadcast its request for an IP address and the local DHCP relay will make the request to a central DHCP server on behalf of the Sun Ray. (See Figure 1.) We plan to move the configuration information to the directory service in the next project stage.

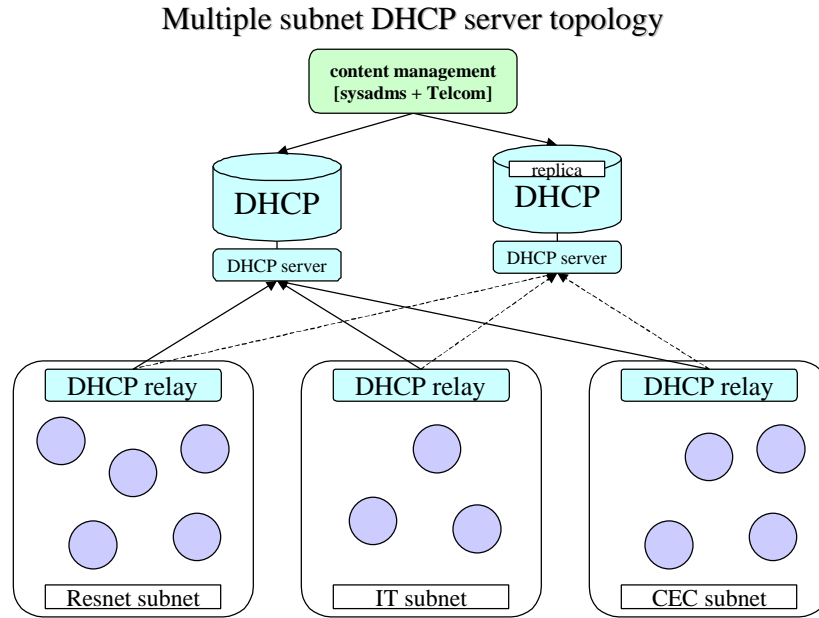


Figure 1

**Medium range strategy**

This project stage is focused on extending the initial applications and services deployed in the previous stage to offering similar functionality over the Internet, implementing encryption, providing enhanced tools for managing accounts, providing an oversight mechanism for and linking additional applications to the directory service, and piloting LDAP-based authentication. Target completion date for this stage is August 1, 2001.

**Deployment constraints**

Due to the high-degree of autonomy that departments have regarding their technical environment, we cannot mandate that they implement specific technologies. As a result, widespread deployment of our recommended authentication system may not be achieved until roughly fall of 2001.

In addition, we expect that insecure protocols will not be completely eliminated by the end of this stage. The project team and the System Administration Council will discuss requirements for, overall importance of, and security issues for applications not using encrypted transmissions.

**Project components**

**Off-campus access to applications and data**

We plan to build on stage 1 efforts to offer similar access to applications and home directories over the Internet. To move to the next stage in our overall plan of providing

the campus access to on-line resources from any location, we will deploy a web-based entrance to department applications and personal files. The requirements include:

- Implementing VPN technologies to offer a secure universal access to campus electronic resources.
- Offering a web gateway with e-mail, calendar, and proxied web browsing capabilities, along with access to Unix and Microsoft Windows applications. We evaluated Sun's WebTop product last year, determined that it fit our needs, and began pursuing the acquisition of it or another product with similar functionality. This software relies on a directory service for deployment and, in our case, authentication.

#### Encrypted data transmission including authentication

The team will facilitate the adoption and deployment of SSH, SSL, or other technologies used for the secure transmission of data and authentication information. We expect that insecure protocols may not be completely removable, however a way to tunnel these through a secure one will be researched and implemented., if possible.

#### Account management and authentication services

We plan to move from NIS to LDAP-based authentication for most applications and environments. To accomplish this, we will implement pluggable authentication modules (PAM) to allow all UNIX machines to authenticate users against the directory server and provide a single password environment where back-end authentication transmissions are encrypted. It also brings us one step closer to a single sign-on environment. To accomplish this, we plan to proceed with the following:

- Pilot and rollout LDAP-based authentication including Library Proxy Service, web applications, and selected department LANs.
- Determine operating procedures for account management, such as expiration, changing, resetting, distribution, and cracking of passwords, lock outs, etc. Develop procedures for compromised passwords. Generate initial passwords.
- Develop and distribute materials to users regarding this new University password and the importance of discretion.
- Design and implement a directory authentication module and password change application.
- Distribute the pluggable authentication modules (PAM) and configuration information to pilot participants. Monitor results and alter package as necessary.
- Implement access-controlled LDAP-based authentication for web sites.
- Deploy a Name Service Switching (NSS) module to group users similar to the way NIS works, again in a UNIX environment. This is an essential component that allows account information to be retrieved from a directory server and provides flexibility for home directories and other account information that may differ across departments.
- Provide enhanced account management tools for system administrators. Preferably these tools will work similarly to those that are used with NIS/YP (i.e., ypwhich, ypcat, etc.). This will ease the learning curve necessary for our system administrators and others that must maintain account information for departments.

#### Oversight mechanism for directory service

Although the benefit of using a centralized LDAP server increases with the number of applications that take advantage of it, the complexity of managing the service also

increases. We will establish a group whose function is to represent the primary stakeholders and keep abreast of changes in the technology, data policy, and other university requirements.

#### Applications linked to directory service

Additional applications we will be linking to the directory include the DHCP service mentioned above, e-mail forwarding, and our internal PBX, and voice mail directory.

### **Long-range strategy**

In the next two to three years, we expect the PKI implementations across higher education and industry to have matured enough to investigate more seriously. Ultimately, government and inter-institutional research applications will drive this implementation at Michigan Tech. At that time, we will implement a new unique identifier to address the need to track the external constituents using our services. However in the interim, we will continue to follow the development of PKI and complete a report outlining our initial stance on it.

We will also continue to link existing applications and build new ones that use directory and authentication services. For example, students will use an array of information appliances, such as web-browsing cell phones or other handhelds, and want secure access to the network from these devices. What kind of policy, standards, and network services must be in place for this to happen?

### **Key deliverables and/or features**

Key deliverables of this effort will be finished by December 2001 and will include:

- Unique identifier strategy and initial implementation.
- Robust production directory service, policy and service oversight group, and resources for developers.
- Authentication strategy and pilot, including central password storage and tools for departmental system administrators to manage their own domains and users.
- Encrypted data transmission utilities deployed and supported.
- Production time services deployed.
- Several campus applications which are useful to a broad range of audiences:
  - PH and finger gateway.
  - Thin client infrastructure.
  - Class rosters with pictures.
  - Modem password kiosk.

### **Evaluation or comparison of competing solutions**

#### **Authentication technologies**

We will be comparing authentication technologies: Kerberos, PKI, and directory services. Our goal is to have one integrated authentication system that can be used for operating systems, network access, and web applications.

## **Directory Service**

Prior to the inception of this project, IT did an analysis of directory servers. We are satisfied with our current system and do not plan to re-evaluate additional products at this time

## **Boundaries and constraints**

### **Staffing**

In the current University budget environment, it is very difficult to acquire new permanent positions for technical support. Adding technical staff to the departments or IT is not realistic. In addition, we want to minimize the load on the technical staff in the academic departments as much as possible.

### **Cost**

IT will leverage the software and hardware cost of this project from existing resources. For deployment there may be some additional costs that will be outlined as a funding request. We understand that the majority of these costs will entail staff time, both from IT and the departments. Also, large increases in services and supplies budgets to support the infrastructure are not realistic.

### **Distributed responsibility for departmental computing**

The process and plan must fit our distributed responsibility environment. We cannot mandate the use of a technology across campus.

### **Robust technology based on standards**

The technologies implemented must be scaleable and robust enough to support the applications we're interested in deploying. The solution must also be standards-based to allow us to change from one product to another with less effort and to integrate implement multiple vendor and/or open source products.

### **Staged approach**

Due to the number and impact of the changes regarding how we approach our data and security models, implementing directory and authentication services must be done in stages. This allows for education among the technical staff and their constituents, and gives the IT organization time to ensure that the new services are robust before they are in full production across campus.

### **Broad representation**

The project team must comprise a broad section of campus, including developers, technical support, data custodians, and potential end-users. The institutional data custodians must be involved in the use and privacy of data. The campus technical community must be involved in the design of the architecture.

## **Role of external specialists or consultants**

In general, we use the information gleaned from other higher educational institutions' experiences to guide our projects and this one is no different. However, we will make use of the Burton Group database of documents and technical briefings for one year to assist us in this deployment. In general, these outside sources offer us information on

- implementation methods and best practices,
- possible pitfalls and methods to avoid them, and
- technical issues and standards.

## Key project issues and risk assessment

There are several critical issues, which could jeopardize the project if they are not addressed in a timely fashion or planned for during the course of the project. However, the greatest risk to the institution is incurred by not implementing these technologies, as noted above in the *Justification and consequences* section. Regarding the project, the main risk factors include:

- **Implementation of a cutting-edge applications infrastructure.** We are participating in the development of middleware best practices for higher education, which may require us to spend additional staff time redoing parts of our implementation as the standard methods evolve.
- **Implementation of the iPlanet directory server.** Even though this product is the industry's vote for best overall directory server, the future of the company remains unknown. We may need to spend additional staff time moving from one directory product to another, if iPlanet has serious business issues.
- **Support from upper administration.** The upper administration must support the overall goals of this project, in order to deflect premature criticism of the project. If we are not given enough time to overcome initial technology and education barriers, we could spend a great deal of effort defending the project and not accomplishing our goals.
- **Support from the department system administrators.** This project, initiated by IT, requires a great deal of education to take place regarding the needs for this infrastructure. Department representatives must be interested in, and benefit from, its deployment. In addition, they must have control over the services they offer to their constituents and the data required to manage them. This entails, for example, allowing technical staff to change user passwords and edit account information. If the departmental system administrators are not behind this project, it could take several years longer to implement due to:
  - Slow deployment of the department-required pieces for implementing the infrastructure.
  - Slow deployment of applications that benefit departments.
  - Miscommunication about the authentication service to their faculty, staff, and students.
- **Support from the institutional data custodians.** If the data custodians are not involved, the trust of the entire middleware deployment could be compromised. In addition, if the Institution unknowingly shares personal data that is protected by FERPA, Michigan Tech could be named in a lawsuit.
- **Staff time to link existing applications to the new infrastructure.** Once the directory service is deployed, there is a danger that we will not move existing applications fast enough to justify its deployment. This could result in questioning the importance of this project and reduction in support across campus for this critical infrastructure.
- **Manageable technologies and architecture.** Due to our staffing restrictions, the technologies and architecture we deploy must be streamlined and automated as much as possible. If it overwhelms our available staff time, we will have little or no time to implement future stages of the project.
- **Robust and secure service.** If the services are not rock-solid, the departments will neither trust, nor use the infrastructure. In addition, if it is not secure, the middleware pieces can be compromised, affect service delivery, and risk data privacy and authenticity.

- **End-user education for long-term deployment of authentication.** At this early stage in the implementation, end-user education will be limited to a discussion on University passwords. Once we consolidate the storage of these passwords and are able to deploy authenticated applications more quickly, the risks will increase when users share their passwords. The users need to practice better password protection.
- **Impact on future projects.** If this middleware project fails, that is, the services we implement are not used, it impacts not only the management of future applications on campus, but also the relationship between IT and the data and technical staff.

## Contingency plan and mitigation measures

Based on the key issues and risks outlined above, the following are our contingency plans and mitigation measures:

- **Implementation of a cutting-edge applications infrastructure.** We have determined that implementing directory services now will provide enough benefit in the short-term that we are willing to do some possible reworking in the future.
- **Implementation of the iPlanet directory server.** Because this product is standards-based, the data and schema can be moved to another standards-compliant directory server with some effort.
- **Support from upper administration.** We will keep the administration informed about the importance and long-term benefit that these technologies have to campus.
- **Support from the departmental system administrators and data custodians.** The contingency plan for these issues depends on where we are in the project and why they are objecting. In essence, our options include:
  - Determine cause(s) and address them.
  - Work on joint projects where the need for middleware can be demonstrated and the applications directly benefit the departments.
- **Staff time to link existing applications to the new infrastructure.** We may enlist other technical staff or hire temporary personnel to assist with this, if necessary.
- **Manageable technologies and architecture.** We may need to hire temporary staff or reduce our project load temporarily until we can either make the case for additional staff or streamline our operations enough to handle this.
- **Offering a robust and secure service.** This is a critical issue that must be planned for addressed from the outset. If the directory service is not available consistently, then we have no option other than to make it so.
- **End-user education for long-term deployment of authentication.** The use of biometrics could mitigate this issue, however access at points without readers would still be problematic.

## Resources

### Human

A campus project team was assembled. (See Appendix A)

### Capital

The budget for the directory services hardware and software is being funded by IT.

## **Space**

Space is available in the Network Operations Center for the deployment of the servers required to support this endeavor.

## **Primary contact person or liaison**

Ann West  
Director of Distributed Computing Services  
Information Technology

## **Project champion or sponsor**

James Cross  
Vice Provost for Information Technology

## **Communication plan**

The communication plan is as follows:

- Present project at a number of forums across campus including user and technical computer committees and data custodian meetings.
- Assemble project team comprising stakeholders across campus that can report back to their areas. Discuss needs and benefits at meetings.
- Establish an e-mail list that is open to anyone at Michigan Tech for subscription. (eateam-1@mtu.edu)
- Develop a web page to inform both on and off campus parties of project status. (<http://www.ea.mtu.edu>)
- Circulate project plans with campus technical and user community
- Discuss the benefits of middleware in other project meetings with campus constituents. Offer code samples or project assistance where appropriate.
- Document successes and application uses.

## Appendix A: Early Adopters Team at Michigan Tech

Name	Title Department
<b>Baker, James/ Walikainen, Dennis</b>	Associate Director, Corporate Relations/ Director, Marketing Communications
<b>Dalquist, Bobbie</b>	Report Designer/Analyst Accounting Services
<b>deBeaubien, Daniel J.</b>	Senior Telecommunications Engineer Telecommunications, IT
<b>Durham, Lee A.</b>	Systems Administrator/Analyst Van Pelt Library
<b>Fredrickson, David J.</b>	Sr. Systems Programmer Administrative Computing, IT
<b>Haapapuro, Marilyn/ Kyllonen, Patty</b>	Associate Director, Human Resources/ Information Specialist, Human Resources
<b>Hale, David D.</b>	System Administrator SAS, IT
<b>Karau, Jarrod</b>	Systems Manager/Administrator Auxiliary Services
<b>Kent, David J.</b>	Sr. Database Administrator Administrative Computing, IT
<b>Piket, Todd C.</b>	Analyst Programmer Distributed Computing, IT
<b>Rothenberger, Viki</b>	Documentation Specialist Telecommunications, IT
<b>Spagnotti, Denise R.</b>	Computer Support Specialist Student Records & Registration
<b>Torrey, Dave</b>	Senior Systems Programmer Center for Experimental Computation
<b>West, Ann</b>	Director Distributed Computing, IT
<b>Willard, George</b>	Sr. Systems Program. Analyst Distributed Computing, IT
<b>Williams, Chris</b>	Sr. System Admin./Manager Mechanical Engineering

